KEY FORMING METHOD AND DEVICE

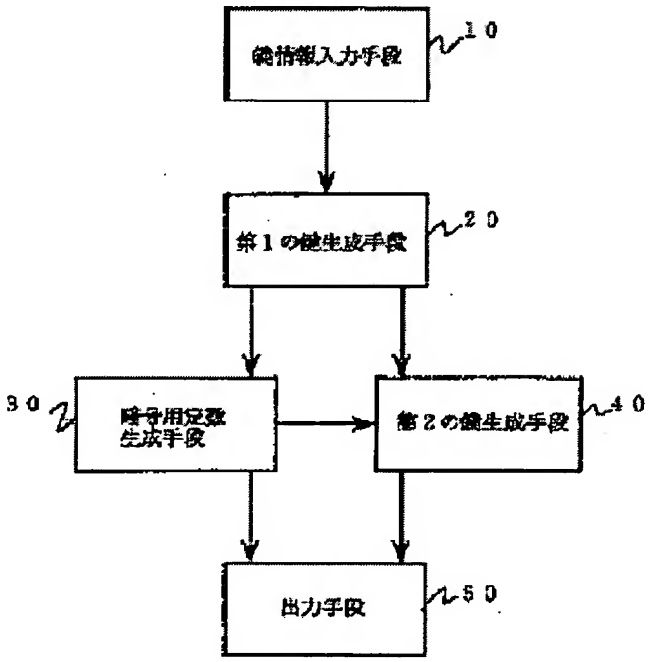
Patent number: JP7121107
Publication date: 1995-05-12

Inventor: MIYAUCHI HIROSHI
Applicant: NIPPON ELECTRIC CO

Classification:
- international: ***G09C1/00; H04L9/00; H04L9/08; H04L9/10; H04L9/12; H04L9/30;*** **G09C1/00; H04L9/00; H04L9/08; H04L9/10; H04L9/12; H04L9/28;** (IPC1-7): G09C1/00; H04L9/00; H04L9/10; H04L9/12
- european:
Application number: JP19930270709 19931028
Priority number(s): JP19930270709 19931028

Abstract of **JP7121107**

PURPOSE:To enable the utilization of a key arbitrarily desired by a user for either of a privacy key or public key by forming such a constant for a cipher to make a first key as a just key and forming a second key corresponding to the first key.
CONSTITUTION:A key information input means 10 is inputted with the information for forming the first key and sends the inputted key information to a first key forming means 20. The first key forming means 20 forms the first key by subjecting the number obtd. from the numerical value of the key information or the key information to predetermined conversion. A constant forming means 30 for cipher receives the first key from the first key forming means 2 and forms the constant for the cipher in such a manner that the first key is the just key. A second key forming means 40 receives the first key from the first key forming means 20 and the constant for the cipher from the constant forming means 30 for the cipher and forms the second key for the first key. An output means 50 receives the constant for the cipher from the constant forming means 30 for the cipher and the second key from the second key forming means 2 and outputs the received constant and key.



(19) 日本国特許庁 (JP)　　(12) 公開特許公報（A）　　(11) 特許出願公開番号

特開平７－１２１１０７

(43) 公開日　平成 7年 (1995)5 月 12 日

(51)Int.Cl.[6]		識別記号	庁内整理番号	F I	技術表示箇所
G09C	1/00		9364 －5L		
H04L	9/00				
	9/10				
	9/12				
				H04L 9/00 Z	

審査請求　有　請求項の数 2　OL　（全 4 頁）

(21) 出願番号　特願平5-270709

(22) 出願日　平成 5年 (1993)10 月 28 日

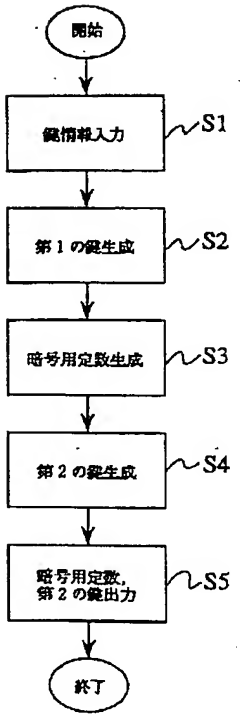
(71) 出願人　000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72) 発明者　宮内　宏
東京都港区芝五丁目7番1号　日本電気株式会社内

(74) 代理人　弁理士　京本　直樹　（外2名）

(54)【発明の名称】鍵生成方法および装置

(57)【要約】
【目的】　鍵と暗号用定数に成立すべき条件がある公開鍵暗号系を用いる際に、秘密鍵、公開鍵の一方をユーザが指定できる方法および装置を提供する。
【構成】　第１の鍵（秘密鍵または公開鍵）のもととなる情報を入力し（Ｓ１）、この情報にあらかじめ定められた変換を施して暗号方式に適合するように第１の鍵を生成する（Ｓ２）。次に、この第１の鍵が正当な鍵になるような暗号用定数生成し（Ｓ３）、これらの暗号用定数を用いて第１の鍵に対応する第２の鍵を生成し（Ｓ４）、暗号用定数と第２の鍵を出力する（Ｓ５）。



【特許請求の範囲】

【請求項１】　公開鍵暗号のための鍵を生成する方法において、第１の鍵のもととなる情報を入力し、該情報にあらかじめ定められた交換を施して第１の鍵を生成し、この第１の鍵が正当な鍵になるような暗号用定数を生成し、前記第１の鍵を対応する第２の鍵を生成し、前記暗号用定数と第２の鍵を出力することを特徴とする公開鍵生成方法。

【請求項２】　公開鍵暗号のための鍵を生成する装置において、第１の鍵のもととなる情報を入力する手段と、該情報を入力して予め定められた変換を施して第１の鍵を生成する手段と、第１の鍵を入力して該第１の鍵が正当な鍵になるような暗号用定数を生成する手段と、暗号用定数および第１の鍵を入力し第１の鍵に対応する第２の鍵を生成する手段と、暗号用定数および第２の鍵を出力する手段と、を具備することを特徴とする公開鍵生成装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、鍵と暗号用定数に成立すべき条件がある公開鍵暗号系を用いる際の、秘密鍵、公開鍵、暗号用定数の組を生成する生成方法および生成装置に関する。

【０００２】

【従来の技術】公開鍵暗号系を利用するにあたっては、暗号鍵、復号鍵の他に、定数が必要になる。例えば、代表的な公開鍵暗号であるＲＳＡ暗号では、暗号鍵ｅ、復号鍵ｄ、定数ｐ，ｑが必要である。ここで、ｐ，ｑは素数であり、ｎ＝ｐ・ｑにて算出されるｎが、暗号に関わるすべての剰余演算の法になる。公開鍵暗号系およびＲＳＡ暗号については、池野信一、小山謙二著「現代暗号理論」にくわしく説明されている。

【０００３】

【発明が解決しようとする課題】ＲＳＡ暗号では、鍵ｋ（ｄまたはｅ）とｐ，ｑのあいだに、

ｋと（ｐ－１）（ｑ－１）は互いに素

という条件が成立することが必須である。従来、ｐ，ｑを先に決定してこれに適合するｅ，ｄを作成する方法がとられているが、この方法ではｅ，ｄを自由に選ぶことはできない。

【０００４】このように、鍵と定数が特定の条件を満たさなければならない公開鍵暗号系では、公開鍵、秘密鍵は両方とも特別な意味のない数値となる。このため、ユーザが秘密鍵を記憶するのが困難になり、ＩＣカードなどに保持する必要がある。

【０００５】本発明は、秘密鍵と公開鍵の一方にユーザが任意に選んだ鍵を利用できるように、暗号用手数、公開鍵を生成する方法および装置を提供する。

【０００６】

【課題を解決するための手段】本発明の鍵生成方法は、

第１の鍵のもととなる情報を入力し、該情報にあらかじめ定められた変換を施して第１の鍵を生成し、この第１の鍵が正当な鍵になるような暗号用定数を生成し、前記第１の鍵の対応する第２の鍵を生成し、前記暗号用定数と第２の鍵を出力することを特徴とする。

【０００７】本発明の鍵生成装置、第１の鍵のもととなる情報を入力する手段と、該情報を入力して予め定められた変換を施して第１の鍵を生成する手段と、第１の鍵を入力して該第１の鍵が正当な鍵になるような暗号用定数を生成する手段と、暗号用定数および第１の鍵を入力して第１の鍵に対応する第２の鍵を生成する手段と、暗号用定数および第２の鍵を出力する手段と、を具備することを特徴とする。

【０００８】

【作用】従来技術では、暗号用定数を先に決定し、これと適合する秘密鍵、公開鍵を生成していたため、秘密鍵として取り得る値に制限があった。しかし、鍵と定数がある条件を満たせばよいのであるから、先に秘密鍵または公開鍵を決定し、これに適合する定数を生成すれば、秘密鍵、公開鍵の一方には任意の鍵を利用することが可能になる。以下では、ＲＳＡ暗号を例として説明する。

【０００９】ＲＳＡ暗号では、鍵ｋ（暗号鍵ｅおよび暗号復号鍵ｄ）と定数として用いる素数ｐ，ｑの間に

ｋと（ｐ－１）（ｑ－１）は互いに素

が成立することが必要である。ｐ，ｑを先に決めるとｋとして任意の鍵を利用することはできなくなる。しかし、ｋを先に決めて、ｋと（ｐ－１），（ｑ－１）が素になるようにｐ，ｑを決定すれば、ｋを利用することができる。

【００１０】秘密鍵として、ユーザが決定する数値、文字列を数値化したもの、などを用いれば、暗証番号やパスワードと同様に利用することができて便宜がはかれるのであるが、ここには問題がある。

【００１１】例えばＲＳＡ暗号の場合、ｐ，ｑは大きな素数であるから、（ｐ－１），（ｑ－１）はいずれも偶数になる。もしも、ユーザが選んだ数値が偶数であったら、これと（ｐ－１），（ｑ－１）は互いに素になりえない。

【００１２】このように、任意の入力数値、入力文字列をそのまま鍵として利用することは必ずしも可能ではない。そこで、本発明では、入力情報に予め定められた変換を施して鍵を作成する方法をとる。例えば、ＲＳＡ暗号の場合には、ユーザが選んだ数値（または、文字列を数値化したもの）が偶数の場合には１を加えるという変換が考えられる。また、（ｐ－１），（ｑ－１）と互いに素になりやすくするため、入力数値に２×３×５×７のような素数の積を掛けてから１を加えるという変換も考えられる。

【００１３】この変換は、入力の数値、文字列に関わらずあらかじめ定めた変換であるから、実際に鍵を利用す

る際も、同様の変換で入力数値、文字列から鍵を生成することが可能である。

【００１４】次に、生成された鍵ｋが正当な鍵になるように暗号用の定数を生成する。ＲＳＡ暗号の場合は、（ｐ－１），（ｑ－１）と互いに素になるような素数ｐ，ｑを作成する。このような素数を作成するためには、例えば、大きな乱数を発生し、これが素数であるかどうかと上記の条件を満たすかどうかをチェックする、という手続きを、暗号用定数の条件を満たすものが得られるまで繰り返すという方法が考えられる。

【００１５】第１の鍵（暗号鍵または復号鍵）ｋと暗号用定数を上記のように生成すれば、第２の鍵（復号鍵または暗号鍵）は、通常の方法に従って生成することができる。例えば、ＲＳＡ暗号の場合には，ｅ，ｄの一方とｐおよびｑからｅ，ｄの他方を、

【００１６】

【数１】

$$ed \equiv 1 \pmod{L}$$

【００１７】に従って作成する。ここでＬは（ｐ－１）と（ｑ－１）の最小公倍数である。本発明では、これらの原理を用いて暗号用定数および鍵を生成する。

【００１８】

【実施例】図１は第１および第２の発明を説明するための処理の流れを示す図である。図２は第２の発明の実施例の構成を表すブロック図である。以下、これらの図を用いて第１および第２の発明を説明する。

【００１９】鍵情報入力手段１０は、第１の鍵を作成するための情報を入力する。この情報は、数値であってもよいし、文字列であっても良い。鍵情報入力手段１０は、入力した鍵情報を第１の鍵生成手段２０へ送る。（図１ステップＳ１）

第１の鍵生成手段２０は、鍵情報入力手段１０から鍵情報を受けとる。鍵情情報が文字列の場合は、これを数値に変換する。この場合、文字コードをそのまま数値として扱うこともできる。第１の鍵生成手段２０は、鍵情報の数値または鍵情報から得られた数に、あらかじめ定められた変換をほどこして第１の鍵を生成する。第１の鍵生成手段２０は、生成された第１の鍵を暗号用定数生成手段３０と第２の鍵生成手段４０に送る。（図１ステップＳ２）

暗号用定数生成手段３０は、第１の鍵生成手段２０から第１の鍵を受けとり、この第１の鍵が正当な鍵になるように暗号用の定数を生成する。暗号用定数生成手段３０は、生成された定数を第２の鍵生成手段４０と出力手段５０に送る。（図１ステップＳ３）

第２の鍵生成手段４０は、第１の鍵生成手段２０から第１の鍵を、暗号用定数生成手段３０から暗号用定数を受けとり、第１の鍵に対応する第２の鍵を生成する。第２の鍵生成手段４０は、生成された第２の鍵を出力手段５０に送る。（図１ステップＳ４）

出力手段５０は、暗号用定数生成手段３０から暗号用定数を、第２の鍵生成手段４０から第２の鍵を受けとり、これらを出力する。（図１ステップＳ５）

【発明の効果】本発明によれば、公開鍵暗号における秘密鍵、公開鍵のいずれか一方をユーザが指定することができる。秘密鍵をユーザが指定する場合には、ユーザが記憶できる数値または文字列を秘密鍵として用いることができるので、鍵をＩＣカード等の媒体に記録しておく必要がなくなり、コストダウン、利便性の向上がもたらされる。一方、公開鍵をユーザが指定する場合には、そのユーザから容易に導き得る数値や文字列（例えば、名前、ユーザ番号、電話番号など）を公開鍵として用いることができるため、公開鍵簿が不要になるか、簡便なもので済むという効果がえられる。

【図面の簡単な説明】

【図１】第１および第２の発明の処理の流れを示す図。

【図２】第２の発明のブロック図である。

【符号の説明】

１０　鍵情報入力手段

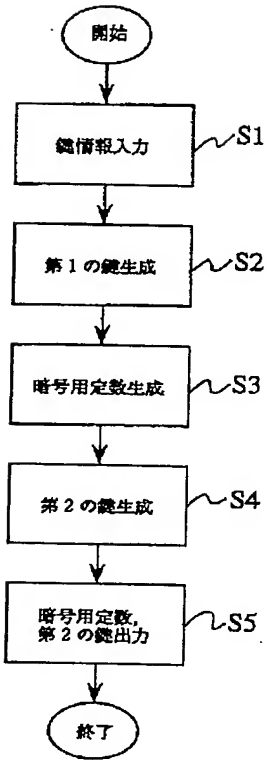
２０　第１の鍵生成手段

３０　暗号用定数生成手段

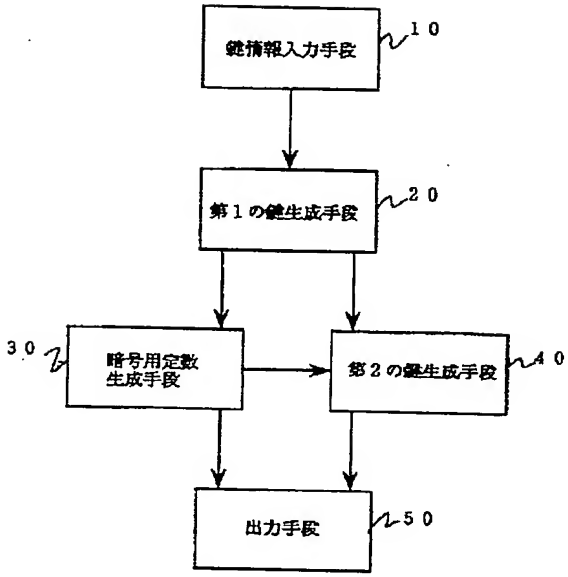
４０　第２の鍵生成手段

５０　出力手段

【図1】


開始
鍵情報入力
S1
第1の鍵生成
S2
暗号用定数生成
S3
第2の鍵生成
S4
暗号用定数，
第2の鍵出力
S5
終了

【図2】


鍵情報入力手段
10
第1の鍵生成手段
20
30
暗号用定数
生成手段
第2の鍵生成手段
40
出力手段
50